Document made available under the Patent Cooperation Treaty (PCT)

International application number: PCT/JP05/016686

International filing date: 05 September 2005 (05.09.2005)

Document type: Certified copy of priority document

Document details: Country/Office: JP
Number: 2004-258186
Filing date: 06 September 2004 (06.09.2004)

Date of receipt at the International Bureau: 20 October 2005 (20.10.2005)

Remark: Priority document submitted or transmitted to the International Bureau in compliance with Rule 17.1(a) or (b)

World Intellectual Property Organization (WIPO) - Geneva, Switzerland
Organisation Mondiale de la Propriété Intellectuelle (OMPI) - Genève, Suisse

日　本　国　特　許　庁
JAPAN PATENT OFFICE

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出　願　年　月　日 Date of Application:	２００４年　９月　６日
出　願　番　号 Application Number:	特願２００４－２５８１８６
パリ条約による外国への出願に用いる優先権の主張の基礎となる出願の国コードと出願番号 The country code and number of your priority application, to be used for filing abroad under the Paris Convention, is	ＪＰ２００４－２５８１８６
出　願　人 Applicant(s):	ソニー株式会社

２００５年　９月２１日

特許庁長官
Commissioner,
Japan Patent Office

中　嶋　誠

【書類名】　特許願
【整理番号】　0390770004
【特記事項】　特許法第３６条の２第１項の規定による特許出願
【提出日】　平成16年 9月 6日
【あて先】　特許庁長官殿
【国際特許分類】　G06F 7/58
【発明者】
【住所又は居所】　東京都品川区北品川６丁目７番３５号　ソニー株式会社内
【氏名】　ミオドラッグ　ミハイエビッチ
【発明者】
【住所又は居所】　東京都品川区北品川６丁目７番３５号　ソニー株式会社内
【氏名】　阿部　譲司
【特許出願人】
【識別番号】　000002185
【氏名又は名称】　ソニー株式会社
【代表者】　安藤　国威
【連絡先】　知的財産部　０３－５４３５－３９０９
【手数料の表示】
【予納台帳番号】　005094
【納付金額】　26,000円
【提出物件の目録】
【物件名】　外国語特許請求の範囲　1
【物件名】　外国語明細書　1
【物件名】　外国語図面　1
【物件名】　外国語要約書　1

【書類名】　翻訳文提出書
【整理番号】　0390770004
【提出日】　平成16年11月 8日
【あて先】　特許庁長官　殿
【出願の表示】
　【出願番号】　特願2004-258186
【特許出願人】
　【識別番号】　000002185
　【氏名又は名称】　ソニー株式会社
　【代表者】　安藤　国威
【確認事項】　本書に添付した翻訳文は、外国語書面出願の願書に添付して提出した外国語明細書、外国語図面及び外国語要約書に記載した事項を過不足なく適正な日本語に翻訳したものである。
【提出物件の目録】
【物件名】　外国語特許請求の範囲の翻訳文　1
【物件名】　外国語明細書の翻訳文　1
【物件名】　外国語図面の翻訳文　1
【物件名】　外国語要約書の翻訳文　1

【書類名】特許請求の範囲
【請求項１】
擬似乱数シーケンスを生成する装置において、
より高いランダム性を有する第１のシーケンスを生成する第１のタイプのセルオートマトンと、
周期について予め定めた下限を有する第２のシーケンスを生成する第２のタイプのセルオートマトンと、
前記第１のシーケンスおよび前記第２のシーケンスに対してビット毎のｍｏｄ２の和を求める加算器とを備えること
を特徴とする装置。
【請求項２】
前記第１のタイプのセルオートマトンは、二次元セルオートマトンであり、
前記第２のタイプのセルオートマトンは、２ＸＬセルオートマトンであり、
前記加算器の合計結果は、前記擬似乱数シーケンスとして出力されること
を特徴とする請求項１に記載の装置。
【請求項３】
対応するセル制御ワードおよび／またはルール制御ワードに基づいて状態が計算され得るセルを有し、第３のシーケンスを生成する第３のタイプのセルオートマトンをさらに備え、
前記セル制御ワードは、前記第２のタイプのセルオートマトンにより生成され、
前記ルール制御ワードは、前記第１のタイプのセルオートマトンにより生成され、
前記加算器は、前記第１、第２および第３のシーケンスのビット毎のｍｏｄ２の和を得ること
を特徴とする請求項１に記載の装置。
【請求項４】
前記加算器の合計結果は、前記擬似乱数シーケンスとして出力されること
を特徴とする請求項３に記載の装置。
【請求項５】
前記加算器からの合計結果に対し非線形マッピングを行なうブロックと、
前記非線形マッピングの結果に対して不均一な間引きを行なうブロックとをさらに備え、
前記間引き結果が前記擬似乱数シーケンスとして出力されること
を特徴とする請求項２また請求項４に記載の装置。
【請求項６】
前記ブロックの各々が、少なくとも１つの非線形関数を含むこと
を特徴とする請求項５に記載の装置。
【請求項７】
前記非線形マッピングを行なうブロックは、ラテン方格（Latin square）に基づいた非線形マッピング用の参照テーブルを少なくとも１つ含むこと
を特徴とする請求項５に記載の装置。
【請求項８】
暗号処理を行なう装置において、
擬似乱数シーケンスを用いてデータを暗号化する暗号プロセッサと、
前記擬似乱数シーケンスを生成する擬似乱数シーケンス生成器とを備え、
前記擬似乱数生成器は、請求項１乃至７のいずれかに記載の装置を含んで構成されること
を特徴とする装置。
【請求項９】
セルオートマトンを用いて擬似乱数シーケンスを生成する方法において、
より高いランダム性を有する第１のシーケンスを生成するステップと、

周期について予め定めた下限を有するた第２のシーケンスの生成するステップと、
前記第１のシーケンスおよび前記第２のシーケンスのビット毎のｍｏｄ２の和を得るステップとを備えていること
を特徴とする方法。
【請求項１０】
セルオートマトンを用いて擬似乱数シーケンスを生成する方法をコンピュータに実行させるコンピュータプログラムにおいて、
前記方法は、
より高いランダム性を有する第１のシーケンスを生成するステップと、
周期について予め定めた下限を有するた第２のシーケンスの生成するステップと、
前記第１のシーケンスおよび前記第２のシーケンスのビット毎のｍｏｄ２の和を得るステップとを備えていること
を特徴とするコンピュータプログラム。
【請求項１１】
セルオートマトンを用いて擬似乱数シーケンスを生成する方法をコンピュータに実行させるコンピュータプログラムを格納する記録媒体において、
前記方法は、
より高いランダム性を有する第１のシーケンスを生成するステップと、
周期について予め定めた下限を有するた第２のシーケンスの生成するステップと、
前記第１のシーケンスおよび前記第２のシーケンスのビット毎のｍｏｄ２の和を得るステップとを備えていること
を特徴とする記録媒体。

【書類名】明細書
【発明の名称】セルオートマトンに基づく、制御可能な周期を有する擬似乱数シーケンスの生成方法および装置
【技術分野】
【０００１】
本発明は、コンパクトな有限状態機械を用いて、制御可能な周期を有する擬似乱数シーケンスを生成する方法および装置に関する。
【背景技術】
【０００２】
近年、セルオートマトンの利用に基づいた、極めて良好な統計特性を備えた擬似乱数シーケンスの生成方法が多く報告されている。例えば、非特許文献１は、高品質乱数を生成する二次元のセルオートマトンを開示している。以下に、典型的な二次元のセルオートマトン（２Ｄ－ＣＡ）について説明する。
【０００３】
セルオートマトン（ＣＡ）は、空間と時間が互いに離散している動的システムである。セルオートマトンは、局所近傍則（local interaction rule）に従ったセルアレイ（cellular array）から構成される。セルの各々は、離散した時間ステップで同期更新されるもので、取りうる有限数の状態のうちの１つとなることができる。ここでは、セルの状態が$s_i \in \{0,1\}$となるブーリアンオートマトンだけを考慮するものとする。次のステップにおけるセルの状態は、周辺近傍セルの現在の状態によって決定される。
【０００４】
セルアレイ（グリッド）はｄ次元で、実用に際してはｄ＝１，２，３が使用される。本明細書のこのセクションでは、ｄ＝２、つまり二次元のグリッドが考慮される。
【０００５】
各セルに含まれているルールは、本質的に有限状態機械ルールであって、通常はルール・テーブル（遷移関数としても知られている）の形で特定されており、状態に関して可能性のある近傍配置すべてについてのエントリを含んでいる。１つのセルのセル近傍構造（neighborhood）は、それ自体および周囲の（隣接する）セルからなる。一次元のＣＡについては、セルは、いずれか一方の側でｒのローカルな近傍（セル）に接続される。ここで、ｒは半径と呼ばれるので、各セルは２ｒ＋１の近傍を有する。
【０００６】
二次元ＣＡ（２Ｄ－ＣＡ）については、２つのタイプのセル近傍が通常考慮される。これらは次のとおりである：その直近の非対角線の４つの近傍（フォンノイマンの近傍としても知られている）及び当該セルからなる５つのセルと、その周囲の８つの近傍及び当該セルからなる９つのセル（ムーアの近傍としても知られている）とがある。
【０００７】
有限のサイズのグリッドを考慮する場合、周期的な境界条件が良く使われ、一次元の場合には円形状グリッド（circular）に、二次元の場合には環状体（toroidal）のものとなる。また、固定あるいはヌル（null）の境界条件も使用することもできる。この場合、グリッドは固定した状態あるいは０（零）の状態にあるセルからなる外部層で囲まれる。後者の場合、通常、ハードウェアで実施するのが容易である。
【０００８】
不均一の（あるいは異質）セルオートマトンは、均質なのものと同じ方法で機能するが、唯一の相違点は、セルルールをすべてのセルに対して同一とする必要がないということである。不均一のＣＡも、均質のものと同様に、基本的で有利な特性、即ち単純性、並行性（parallelism）およびローカル性を共有する。
【０００９】
２Ｄ－ＣＡについての適切な背景的考察は、例えば非特許文献２に開示されている。
【００１０】
【非特許文献１】M. Tomassini, M. Sipperand, M. Perrenoud, "On the generation

of high-quality random number by two-dimensional cellular automata"「二次元のセルオートマトンによる高品質乱数の生成について」, IEEE Trans. Computers, vol. 49, pp. 1146-1151, Oct. 2000

【００１１】

【非特許文献２】P. P. Chaudhuri, D. R. Chaudhuri, S. Nandiand, S. Chattopadhyay, "Additive Cellular Automata: Theory and Applications"「加法的セルオートマトン：理論および応用」, NewYork, IEEE Press, 1997.

【非特許文献３】S. Wolfram, "Cryptography with Cellular Automata"「セルオートマトンによる暗号法」, Advances in cryptology - CRYPTO85, Lecture Notes in Computer Science, vol. 218, pp. 429-432, 1985

【非特許文献４】K. Cattell, S. Zhang, M. Serraand, J. C. Muzio, "2-by-n hybrid cellular automata with regular configuration: Theory and application"「規則的な配置を備えた２×ｎハイブリッドセルオートマトン：理論および応用」, IEEE Trans. Computers, vol. 48, pp. 285-295, March 1999

【非特許文献５】A. Klimov and A. Shamir, "Cryptographic applications of T-functions"「Ｔ－関数の暗号の応用」, SAC'2003, pre-print 15 pages, August 2003, (to appear in Lecture Notes in Computer Science)

【非特許文献６】S.-U. Guan and S. Zhang, "An evolutionary approach to the design of controllable cellular automata: structure for random number generation"「制御可能なセルオートマトン設計への進化したアプローチ：乱数発生用構造」, IEEE Trans. Evolutionary Computation, vol. 7, pp. 23-36. Feb. 2003.

【非特許文献７】P. D. Hortensius, R. D. Mcleod, W. Pries, D. M. Miller and H. C. Card, "Cellular automata-base pseudorandom number generators for built-in self-test"「セルオートマトンに基づく、ビルトイン・セルフテスト用の擬似乱数生成器」, IEEE Transactions on Computer-Aided Design, vol. 8, pp. 842-859, August 1989.

【非特許文献８】M. Mihaljevic, M. P. C. Fossorier and H. Imai, "Fast correlation attack algorithm with the list decoding and an application"「リスト符号解読およびアプリケーションを備えた高速相関性攻撃アルゴリズム」, FSE2001, Lecture Notes in Computer Science, vol. 2355, pp. 196-210, 2002.

【非特許文献９】N. T. Courtois and W. Meier, "Algebraic attacks on stream ciphers with linear feedback"「線形フィードバックによるストリーム暗号への代数的攻撃」, EURO-CRYPT2003, Lecture Notes in Computer Science, vol. 2656, pp. 345-359, 2003.

【非特許文献１０】M. Mihaljevic and H. Imai, "A family of fast keystream generators based on programmable linear cellular automata over GF(q) and time variant table"「ＧＦ（ｑ）および時間変化テーブルに対するプログラム可能な線形のセルオートマトンに基づく、高速キーストリーム生成器のファミリ」, IEICE Transactions on Fundamentals, vol. E82-A, pp. 32-39, Jan. 1999.

【非特許文献１１】G. Marsaglia, "Diehard"「ダイハード」(1998). http://stat.fsu.edu/geo/diehard.htm.

【非特許文献１２】A. K. Das, A. Ganguly, A. Dasgupta, S. Bhawmik, and P. Pal Chaudhuri, "Efficient characterization of cellular automata", 「セルオートマトンの効率的な特性」, IEE Proc. Pt. E, vol. 137, pp. 81-87, Jan. 1990.

【非特許文献１３】K. Cattell and J.C. Muzio, "Synthesis of one-dimensional linear hybrid cellular automata"「一次元線形ハイブリッド・セルオートマトンの合成」, IEEE Trans. Computer-Aided Design, vol. 15, pp. 325-335, March 1996.

【非特許文献１４】S. Nandi, B. K. Kar and P. Pal Chaudhuri, "Theory and applications of cellular automata in cryptography"「暗号法でのセルオートマトンの理論および応用」, IEEE Trans. Comput., vol. 43, pp. 1346-1357, Dec. 1994.

【非特許文献１５】W. Meier and O. Staffelbach, "Analysis of pseudo random sequences generated by cellular automata"「セルオートマトンによって生成された擬似乱数シーケンスの分析」, Advances in Cryptology - EUROCRYPT 91, Lecture Notes in Computer Science, vol. 547, pp. 186-189, 1992.
【非特許文献１６】C. K. Koc and A.M. Apohan, "Inversion of cellular automata iterations"「セルオートマトン反復の転位」, IEE Proc. Comput. Digit. Tech., vol. 144, pp. 279-284, 1997.
【非特許文献１７】M. Mihaljevic, "An improved key stream generator based on the programmable cellular automata"「プログラム可能なセルオートマトンに基づいた、改良キーストリーム生成器」, ICICS'97, Lecture Notes in Computer Science, vol. 1334, pp. 181-191, 1997.
【非特許文献１８】M. Mihaljevic, "Security examination of a cellular automata based pseudorandom bit generator using an algebraic replica approach"「代数的複製アプローチを使用する、セルオートマトン・ベースの擬似乱数ビット生成器のセキュリティ試験」, AAECC12, Lecture Notes in Computer Science, vol. 1255, pp. 250-262, 1997.
【非特許文献１９】S.R. Blackburn, S. Murphy and K.G. Peterson, "Comments on "Theory and Applications of Cellular Automata in Cryptography""「『暗号法でのセルオートマトンの理論および応用』に関するコメント」, IEEE Trans. Comput., vol. 46, pp.637-638, May 1997.
【非特許文献２０】M. Mihaljevic, "Security examination of a cellular automata based pseudorandom bit generator using an algebraic replica approach"「代数的複製アプローチを使用する、セルオートマトン・ベースの擬似乱数ビット生成器のセキュリティ試験」, AAECC12, Lecture Notes in Computer Science, vol. 1255, pp. 250-262, 1997.
【非特許文献２１】A. J. Menezes, P. C. van Oorschot and S. A. Vanstone, Handbook of Applied Cryptography（応用暗号法ハンドブック）. Boc. Roton: CRC Press, 1997.

【発明の開示】

【発明が解決しようとする課題】

【００１２】

しかしながら、上述の提案の主な欠点は、生成された擬似乱数シーケンスの周期に関して保証がないことである。従って、上述したような望ましい統計特性のランダム性を備えた、最大または実質的に最大周期のシーケンスを生成するための方法と装置を提供することが望ましい。

【００１３】

本発明は上記を考慮してなされている。本発明の目的は、制御可能な周期を有する、所望の擬似乱数シーケンスを生成する方法および／またはコンパクトな装置を提供することにある。

【課題を解決するための手段】

【００１４】

本発明の一実施形態によれば、擬似乱数シーケンス生成装置が提供される。本装置は、より高いランダム性を有する第１のシーケンスを生成する第１のタイプのセルオートマトンと、周期について予め定めた下限を有する第２のシーケンスを生成する第２のタイプのセルオートマトンと、前記第１のシーケンスおよび前記第２のシーケンスに対してビット毎のｍｏｄ２の和を求める加算器とを備えることを特徴とする。

【００１５】

本実施形態による装置では、前記第１のタイプのセルオートマトンは、二次元セルオートマトンであってもよく、前記第２のタイプのセルオートマトンは、２×Ｌセルオートマトンであってもよい。また、前記加算器からの合計結果は、擬似乱数シーケンスとして出

力され得る。

【００１６】

本発明の他の実施形態によれば、上述した装置において、第３のシーケンスを生成するための第３のタイプのセルオートマトンをさらに備えていてもよい。前記第３のタイプのセルオートマトンは、対応するセル制御ワードおよび／またはルール制御ワードに基づいて、状態が計算され得るセルを有する。本実施形態では、前記セル制御ワードは、前記第２のタイプのセルオートマトンによって生成され、前記ルール制御ワードは、前記第１のタイプのセルオートマトンによって生成され、前記加算器は、前記第１、第２および第３のシーケンスのビット毎のｍｏｄ２の和を得る。

【００１７】

本発明のさらに他の実施形態によれば、上述した装置において、前記加算器からの合計結果に非線形マッピングを行なうブロックと、該非線形マッピングの結果について不均一な間引きを行なうブロックとをさらに備え、前記間引き結果が前記擬似乱数シーケンスとして出力されてもよい。本装置では、前記ブロックの各々が、少なくとも１つの非線形関数を含んでいてもよい。あるいは、前記非線形マッピングを行なうブロックは、ラテン方格（Latin square）に基づいた非線形マッピング用参照テーブルを少なくとも１つ含んでもよい。

【００１８】

本発明の他の実施形態によれば、暗号処理を行なう装置が提供される。本装置は、擬似乱数シーケンスを用いてデータを暗号化する暗号プロセッサと、前記擬似乱数シーケンスを生成する擬似乱数シーケンス生成器とを含むことを特徴とする。本実施形態では、前記擬似乱数生成器は、上記実施形態のうちの任意の１つによる装置を含むように構成される。

【００１９】

本発明の他の実施形態によれば、セルオートマトンを用いて擬似乱数シーケンスを生成する方法、または該方法をコンピュータに実行させるコンピュータプログラム、または該コンピュータプログラムを格納する記録媒体が提供される。前記方法は、より高いランダム性を有する第１のシーケンスを生成するステップと、周期について予め定めた下限を有するた第２のシーケンスの生成するステップと、前記第１のシーケンスおよび前記第２のシーケンスのビット毎のｍｏｄ２の和を得るステップとを備えている。

【発明の効果】

【００２０】

本発明によれば、制御可能な周期を有する所望の擬似乱数シーケンスの生成方法および／またはコンパクトな装置が提供される。

【発明を実施するための最良の形態】

【００２１】

第１の実施形態：

本発明の第１の実施形態によれば、コンパクトな有限状態機械（finite state machine）を用いて、制御可能な周期を有する擬似乱数シーケンスを生成する方法および装置が提供される。本実施形態による装置は、セルオートマトンの２つの異なるクラスに基づくものである。本装置および本方法は、フレキシブルであり、空間複雑度とシーケンス周期の下限の間のトレードオフ(trade-off)についての好機を与えるものである。

【００２２】

本発明の第１の実施形態について説明する前に、セルオートマトンに関する基礎技術のうち、本実施形態で使用されるいくつかの技術について、添付図面を参照して説明する。

【００２３】

基本的なバイナリ・セルオートマトン（Basic Binary Cellular Automata）：

一次元のバイナリ・セルオートマトン（ＣＡ）は、直列接続された、０あるいは１の値をとるＬ個のセルアレイと、ｑ個の変数を有するブール関数ｆ（ｘ）の値とから構成される。セルx_iの値は、ｉ＝１，２，．．．，Ｌについて、$x'_i = f(x)$として、離散

時間ステップでこの関数を使用して、パラレルに（同期して）更新される。境界条件は、通常、指標値モジュールＬをとることにより処理される。パラメータｑは、通常、奇数の整数（つまりｑ＝２ｒ＋１）であり、ここでｒは、関数ｆ（ｘ）の半径としばしば呼ばれる。ｉ番目のセルの新しい値は、ｉ番目のセルの値、およびｉ番目のセルの左右ｒ個近傍のセルの値を使用して計算される。

【００２４】

各々が０または１の値をとるＬ個のセルがあるので、2^L個の可能な状態ベクトルがある。S_kで、時間ステップｋでの状態ベクトルを表わすものとする。初期状態ベクトルS_0からスタートして、セルオートマトンは、時間ステップｋ＝１；２；３；．．．などで、状態S_1，S_2，S_3などに移る。状態ベクトルS_kは、ｋが進むにつれて、Ｌビットのバイナリ・ベクトルの群（セット）から値をとり、状態マシンは結果として循環する。つまり、以前（$S_k=S_{k+P}$）に到達した状態S_{k+P}に達する。この周期Ｐは、初期状態、更新機能およびセル数の関数である。

【００２５】

ｑ＝３を有するＣＡについては、各離散時間ステップｔ（時計サイクル）でｉ番目のセルの展開は、（ｉ－１）番目、（ｉ）番目、（ｉ＋１）番目セルの現在の状態の関数として表わすことができる。

【００２６】

【数１】

$$x_i(t+1) = \{ f(x_{i-1}(t),\ x_i(t),\ x_{i+1}(t) \} \quad \cdots (1)$$

【００２７】

ｆはＣＡに関連した組合せ論理(combinatorial logic）とも呼ばれる。組合せ論理は、それぞれ次の状態に展開するために更新ルールを表わす。

【００２８】

セルの次の状態関数が真理値表（truth table）の形で表現される場合、真理値表中の出力カラムの１０進の等価は、従来通りにＣＡルール番号と呼ばれる。非特許文献３の中で提案され考慮したルール３０と呼ばれる非線形ルールは、下記によって更新を実現する：

【００２９】

【数２】

$$x_i(t+1) = x_{i-1}(t)\ \mathrm{XOR}\ [\, x_i(t)\ \mathrm{OR}\ x_{i+1}(t)\,] \quad \cdots (2)$$

【００３０】

特に興味深いのはＧＦ（２）に関する２つの線形ルールである。これらは、ルール９０およびルール１５０としてそれぞれ知られている。ルール９０では、以下の組合せ論理に従って、現在から次の状態までの展開（更新）を指定する：

【００３１】

【数３】

$$x_i(t+1) = x_{i-1}(t) \oplus x_{i+1}(t) \quad \cdots (3)$$

【００３２】

ここで、丸に十字の記号（以下「○＋」と略す）はＸＯＲ演算を示す。なお、ルール９０が適用される場合、ｉ番目のセルの次の状態が、その左右の近傍の現在の状態に依存する。同様に、ルール１５０用の組合せ論理は、以下により与えられる：

【００３３】

【数４】

$$x_i(t+1) = x_{i-1}(t) \oplus x_i(t) \oplus x_{i+1}(t) \quad \cdots (4)$$

【００３４】

すなわち、ｉ番目のセルの次の状態は、その左右の近傍の現在の状態およびさらにそれ自身の現在の状態に依存する。

【００３５】

ＣＡでは、同じルールがすべてのセルに適用される場合、ＣＡは均質なＣＡと呼ばれる。そうでなければ、それはハイブリッドＣＡと呼ばれる。様々な境界条件がある場合がある。すなわち、ヌル（端部のセルが論理「０」に接続される場合）、周期的（端部のセルが隣接する）、などである。

【００３６】

ＣＡの背景技術は非特許文献２で見つけることができる。

【００３７】

２×Ｌセルオートマトン（2-by-L Cellular Automata）：

２×Ｌ ＣＡは非特許文献４で提案され考慮されたが、このセクションでは２×Ｌ ＣＡのある特性について簡単に説明する。

【００３８】

上述したように、線形の有限状態機械（ＬＦＳＭ）は、Ｌ個のシングルビット・メモリエレメントおよびｌつの遷移関数で構成される。時間ｔでｉ番目のメモリエレメントの値または状態は、s^t_iで示される。時間ｔのＬＦＳＭの状態は、s^tで示される。遷移関数ｆは、時間ｔの状態から時間ｔ＋ｌでのＬＦＳＭの状態を決定する。すなわち$s^{t+1}=f(s^t)$である。ＬＦＳＭの次の状態関数は、グラフ式に状態図を使用して記述することができる。なお、ＬＦＳＭの直線性は、ｆがｎビット・ベクトルからｎビット・ベクトルまで線形関数であることを意味する。すなわち、任意の２つの状態ａおよびｂについて

$$f(a+b)=f(a)+f(b)$$

である。遷移関数ｆは、ｎ個の関数$f_1, f_2, \ldots, f_n$として特定することができ、ここで、ｉ番目の関数がセルｉの次の状態を計算する。

【００３９】

$$s_i^{t+1}=f_i(s^t)$$

ＣＡとの関連では、関数f_iは、セルｉについてのセルルールと呼ばれる。f_iの各々が線形の場合、しかもその場合のみ、遷移関数ｆは線形である。簡単のために、ｓが現在の状態を示すために使用され、次の状態にはs^+が使用されるものとする。同様に、s_iは現在の状態を示し、s_i^+はセルｉの次の状態を示すものとする。ＣＡにおいて、「セル間の通信が最近傍で行われる」とは、各セルがその直近の近傍だけに接続されることを意味している。図ｌは、２×ｌ ＣＡの相互接続構造を示す。左端および右端のセルは、それらの左右の入力部（図では省略されている）で定数０入力をそれぞれ有すると仮定する。そのようなＣＡは、規則的な配置を有する２×ｌ ＣＡと呼ばれる。

【００４０】

各時間ステップにおいて、各セルは、そのセルルールを使用して、新しい状態を計算する。異なるセルは異なるルールを使用することができ、ＣＡをハイブリッドとして構成する。さらに、ＣＡが完全に接続されている、すなわち各セルがその近傍の内３つすべてから入力を受け取ると仮定すると、結果として、セルｉについてのセルルールf_iは、下記のうちの１つであることになる：

【００４１】

【数５】

$$f_i(s_l, s_r, s_v, s_s)=s_l \oplus s_r \oplus s_v \quad \text{（セルがルール０を用いた場合）} \qquad \cdots(5)$$

【００４２】

【数６】

$$f_i(s_l, s_r, s_v, s_s) = s_l \oplus s_r \oplus s_v \oplus s_s \quad \text{（セルがルール１を用いた場合）} \quad \cdots(6)$$

【００４３】

ここで、s_l（s_r）は、左（右）近傍の現在の状態を示し、s_vは、縦方向の近傍のそれを示し、s_sは、セルｉ自体の状態を示す。ルール０およびルール１は、それぞれルール９０およびルール１５０をそのまま一般化したもので、背景技術の一次元ＣＡ文献に開示されている。

【００４４】

２つのルールだけしかないため、セルによって使用されるルールは、シングルビットとしてコード化することができる、つまり、「１」はルール１を示し、「０」はルール０を示す。変数$t_1, t_2, \ldots, t_L$および$b_1, b_2, \ldots, b_L$は、セルによって使用されるルールを示すために用いる。簡単のために、$t_1, t_2, \ldots, t_L$に対応して、トップセルは、１からＬまで番号が付けられ、$b_1, b_2, \ldots, b_n$に対応して、ボトムセルは、Ｌ＋１から２Ｌまで番号が付けられる。一般に、ルール・ベクトル［［$t_1, t_2, \ldots, t_n$］，［$b_1, b_2, \ldots, b_n$］］は、与えられた２×１ＣＡを識別するために使用される。

【００４５】

ＬＦＳＭの遷移行列Ｔは、遷移関数を代数的に定義するので、$s^+ = s \cdot T$である。一次元ＣＡの遷移関数は、三重対角（tridiagonal）である。２×１　ＣＡについて、遷移行列は、ブロック構造を持っている。

【００４６】

【数７】

$$T = \begin{bmatrix} T_1 & I \\ I & T_2 \end{bmatrix} \quad \cdots(7)$$

【００４７】

ここで、T_1とT_2がＬ×Ｌの三重対角行列であり、ＩはＬ×Ｌ単位行列である。例えば、２×４　ＣＡについての遷移行列は以下のとおりである：

【００４８】

【数８】

$$T = \left[\begin{array}{cccc|cccc} t_1 & 1 & 0 & 0 & 1 & 0 & 0 & 0 \\ 1 & t_2 & 1 & 0 & 0 & 1 & 0 & 0 \\ 0 & 1 & t_3 & 1 & 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & t_4 & 0 & 0 & 0 & 1 \\ \hline 1 & 0 & 0 & 0 & b_1 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 & 1 & b_2 & 1 & 0 \\ 0 & 0 & 1 & 0 & 0 & 1 & b_3 & 1 \\ 0 & 0 & 0 & 1 & 0 & 0 & 1 & b_4 \end{array}\right] \quad \cdots(8)$$

【００４９】

ここで、t_iおよびb_i（$1 \leqq i \leqq 4$）は上記のように定義される。なお、任意の２×１　ＣＡの遷移行列は対称である。

【００５０】

２×３ＣＡの例を考慮し、ＣＡがルール・ベクトル［［１，１，０］，［０，０，１］］を使用すると仮定すると、その結果は、以下のとおりである。

【００５１】

$[t_1, t_2, t_3] = [1, 1, 0]$ 及び $[b_1, b_2, b_3] = [0, 0, 1]$

s_i $(1 \leqq i \leqq 6)$を現在とすると

【００５２】

【数９】

$$s_1^+ = s_1 \oplus s_2 \oplus s_4$$
$$s_2^+ = s_1 \oplus s_2 \oplus s_3 \oplus s_5$$
$$s_3^+ = s_2 \oplus s_6$$
$$s_4^+ = s_1 \oplus s_5$$
$$s_5^+ = s_2 \oplus s_4 \oplus s_6$$
$$s_6^+ = s_3 \oplus s_5 \oplus s_6$$

【００５３】

最小コストの２×Ｌ－ＣＡ（Minimal Cost 2-by-L CA）：

任意のアプリケーションついて、一般に、ＬＦＳＭインプリメンテーションのハードウェアコストを最小限にすることを試みることが望ましい。１Ｄ ＣＡに関し同様の方法で、５００までの程度で最小コストの２×１ ＣＡが計算されたが、これは、非特許文献４で報告されている。なお、ハードウェアコストを最小限にすることは、ルール１を用いるセル数を最小限にすることを意味する。というのは、ルール１は、評価およびインプリメンテーションについて、わずかに高い複雑度を有するからである。

【００５４】

与えられた２×１ ＣＡが最大長サイクルを持っているかとうか決めるために、非特許文献４で提案されたアルゴリズムは、以下のとおりである：

１．非特許文献４に記述された定理１での回帰関係を使用して、ＣＡの固有多項式を計算する、

２．固有多項式がプリミティブかどうかをチェックし、もしそうであれば、ＣＡは最大長サイクルを有する。

【００５５】

従って、各ｎ（１≦ｎ≦２５０）について、アルゴリズムは、最初に均質なルール０ＣＡを生成しチェックする。これが成功しない場合（その筈はないが）、アルゴリズムは、単一のルール１セルを備えた２×ｎ ＣＡをすべて生成する。これが成功しない場合、アルゴリズムは、１対のルール１セルを有するＣＡをすべて生成する。そしてこれを続けていく。各ｎについて、検索は、最大長サイクルを有する最初の２×ｎ ＣＡで止められた。従って、生成されたＣＡは、最小コストを有する、つまり、最も少ない数のルール１セルを使用する。アルゴリズムの結果は、非特許文献４の表３に示されている。

【００５６】

なお、Ｌ＝２およびＬ＝４については、最大長サイクルの２×ｎ ＣＡが存在しない。２×２ＣＡの構造は、周期的な線形のハイブリッドＣＡと同じである。したがって、最大長マシンがないのは驚くことではない。

【００５７】

非特許文献４中で計算した結果は、均質な重み１ ＣＡに関する２つの観察につながる。セルがすべて同じルールを使用する場合、ＣＡは均質である。そのようなＣＡは、セルがすべてルール０を用いる場合ルール０ＣＡと呼ばれ、あるいは、セルがすべてルール１を使用する場合、ルール１ＣＡと呼ばれる。重み１ＣＡは、ルール１を用いる単一のセルとルール０を使用する全ての残りのセルとを有する。非特許文献４の中で報告された観察は次のとおりである：

・観察１．最大長の均質ＣＡは、存在しない。

・観察２．Ｌ＞１の場合、最大長の重み１ ＣＡは存在しない。

【００５８】
本実施形態による装置および方法：
初めに、制御可能な周期を有する擬似乱数シーケンスを生成する第１の実施形態による方法を説明する。
【００５９】
バイナリのシーケンス$\{a_i\}_i$および$\{b_i\}_i$は、２つの独立プロセスの実現であり、下記が有効であると仮定する。
・シーケンス$\{a_i\}_i$を生成するプロセスは、実験によって評価された少なくとも適度な周期と、統計的テストのシステムで測定された望ましいランダム性特性を有するシーケンスを提供する。
・シーケンス$\{b_i\}_i$を生成するプロセスは、値が分析的に証明可能である長い周期と、統計的テストのシステムで測定された少なくとも適度なランダム性特性を有するシーケンスを提供する。
【００６０】
そして、本出願の発明者は以下が有効であること発見した。
・シーケンス$\{c_i\}_i = \{a_i 「○+」 b_i\}_i$は、値が分析的に証明可能である長い周期と、統計的テストのシステムによって測定された望ましいランダム特性とを有する。
【００６１】
上記の知見によれば、高いランダム性特性および制御可能な周期を有する、バイナリのシーケンスを生成する下記方法が提供され、該方法は以下のステップを含む：
（１）適切なセルオートマトンに基づいたアプローチを使用して、所望のランダム特性および予期された周期の（少なくとも）適度な長さを備えたバイナリのシーケンスを生成するアルゴリズムを特定する；
（２）適切なセルオートマトンに基づいたアプローチを使用して、所望の周期および（少なくとも）適度なランダム特性のバイナリのシーケンスを生成するアルゴリズムを特定する；
（３）上記２つの要素シーケンスのビット毎ｍｏｄ２の和として、結果として生じるシーケンスを生成する；結果的に生じるシーケンスについて予期される特性は、所望の統計特性およびシーケンス周期の制御可能な下限である。
【００６２】
次に、制御可能な周期を有する擬似乱数シーケンスを生成する第１の実施形態による装置の一例について説明する。制御可能な周期の擬似乱数シーケンスを生成する装置のための３つの主な構成要素は次のとおりである：
・図１に表示され、上記セクションおよび表１で特定される２ＸＬ　ＣＡ；
・図２に表示され、表２（詳細に関しては上記セクションを参照）に基づいて特定される２Ｄ－ＣＡ；および
・２ＸＬ．ＣＡおよび２Ｄ－ＣＡから生じるシーケンスのビット毎ｍｏｄ２の和のための加算器。
【００６３】

【表１】

L	２×Ｌ　ＣＡ　仕様
3	1，2，6
32	8，13
64	1，4，46
96	5，10
128	2，226

【００６４】

【表２】

ルール１５	$s_{i,j}(t+1) = s_{i-1,j}(t) \oplus s_{i,j-1}(t) \oplus s_{i+1,j}(t) \oplus s_{i,j+1}(t)$
ルール３１	$s_{i,j}(t+1) = s_{i-1,j}(t) \oplus s_{i,j-1}(t) \oplus s_{i+1,j}(t) \oplus s_{i,j+1}(t) \oplus s_{i,j}(t)$
ルール４７	$s_{i,j}(t+1) = 1 \oplus s_{i-1,j}(t) \oplus s_{i,j-1}(t) \oplus s_{i+1,j}(t) \oplus s_{i,j+1}(t)$
ルール６３	$s_{i,j}(t+1) = 1 \oplus s_{i-1,j}(t) \oplus s_{i,j-1}(t) \oplus s_{i+1,j}(t) \oplus s_{i,j+1}(t) \oplus s_{i,j}(t)$

【００６５】

表１は、複数個の特定の２×Ｌ　ＣＡを特定する。表中のエントリは、どのセルがルール１を使用するか示す。例えばはエントリ

３　　１，２，６

は、２×３ＣＡのルールベクトルを表す。つまり、６つのセルのＣＡについてのルール・ベクトルは

以下の通りとなる。

【００６６】

$[[t_1, t_2, t_3], [b_1, b_2, b_3]] = [[1, 1, 0], [0, 0, 1]]$

ここで、「１」は、セル１、２および６のルール１を示す。

【００６７】

本装置は、高品質の擬似乱数シーケンスを生成する、非特許文献１で報告されている特定の２Ｄ－ＣＡを使用する。これは、二次元（２Ｄ）の８×８の配列に整えられた６４のセルからなる。

【００６８】

ｓｉ，ｊ（ｔ）は、時刻ｔ，ｉ，ｊ＝１，２，．．．．，８に、座標（ｉ，ｊ）を有する２Ｄ－ＣＡのセル状態を示すとする。使用される２Ｄ－ＣＡでは、セルは、表２で与えられるルールのうちの１つに従って更新される。使用される２Ｄ－ＣＡは、図２に示す。

【００６９】

図３は、本発明の第１の実施形態による装置の配置例を示す。本装置は、２Ｄ－ＣＡ３１０、２×Ｌ　ＣＡ３２０、２Ｄ－ＣＡセル出力および対応する２×Ｌ　ＣＡセル出力のビット毎ｍｏｄ２加算を行なう加算器３３０－１，３３０－２，．．．，３３０－ｎ、および生成された高品質の制御可能な周期の擬似乱数シーケンス３５０を出力するために、ｍｏｄ２加算演算結果をバッファするバッファ３４０を有する。ここで、高品質擬似乱数シーケンスとは、シーケンス・ランダム性を測定する指定された統計的なテスト群をパスするシーケンスを意味する。

【００７０】

本装置は、ＣＰＵとメモリを備えたコンピュータに所定のプログラムを実行させたり、あるいは、ハードウェアロジック装置により実現することができる。

【００７１】
図３に示された本装置は、以下のように動作する。
・初期化：独立したランダム・ビットのシーケンスを用いて、すべてのセルを初期化する。
・シーケンス生成：本装置の各サイクルは、次のステップからなる：
（１）２×Ｌ　ＣＡ３２０を１サイクル動作させ、その全てのセルを更新する；
（２）２Ｄ－ＣＡ３１０を１サイクル動作させ、その全てのセルを更新する；
（３）２Ｄ－ＣＡ３１０のセルと対応する２×Ｌ　ＣＡ３２０のセルとのビット毎ｍｏｄ２加算を行なう。
【００７２】
次の表３は、本装置の空間複雑度および出力シーケンス周期の得られた下限の典型的な値を示す。
【００７３】
【表３】

使用されたＣＡセル数	出力シーケンス周期の下限
128	2^{64}
160	2^{96}
160	2^{96}

【００７４】
第２の実施形態：
本発明の第２の実施形態によれば、ストリーム暗号（stream cipher）を設計するための構築ブロックのファミリが提供される。これらの構築ブロックの主な役割は、後段処理に好適な擬似乱数シーケンスを生成することである。これらのシーケンスは、高度なランダム性特性、長い周期を有しており、実用上予測不可能なものである。本実施形態の構築ブロックは、出力擬似乱数シーケンスの所望特性を実現するように組み合わせられた３つの異なるクラスのセル・オートマトンに基づいている。本実施形態のファミリは、広い範囲における特定のインプリメンテーションまたはアプリケーション制約に好適な、あるファミリメンバを選択できるという可能性を与えている。
【００７５】
ストリーム暗号用の適切な基礎的構築ブロックの開発は、良く認識されており、開かれた課題である。極めて最近、非特許文献５で、このトピックへの新たな寄与が報告されており、Ｔ関数に基づいた暗号構築ブロックが研究されている。
【００７６】
しかしながら、その課題に取り組むために異なるアプローチを提供することによって、ユーザーあるいはシステム設計者に、擬似乱数シーケンスを生成する、より柔軟な手段を提供することが望ましい。例えば、セルオートマトンの利用に基づいたストリーム暗号について、適切な構築ブロックを得るために新たなフレームワークを提供することが望ましい。本実施形態について詳細に説明する前に、本実施形態中で使用されるＣＣＡの基礎技術のうちのいくつかについて説明する。
【００７７】
制御可能なセルオートマトン（ＣＣＡ：Controllable Cellular Automata）：
本セクションでは、非特許文献６で紹介された、制御可能なセルオートマトン（ＣＣＡ）の概要を述べる。詳細な説明は非特許文献６に開示されている。ＣＣＡの説明に当たり、ＣＣＡの特性を識別するためにいくつかの点について最初に定義する。
・定義：ＣＣＡは、いくつかのセルの動作（とのようにセルの状態が各サイクルで更新さ

れるか）が、セル制御信号によって制御することができるＣＡである。ルール制御信号と同様に、セル制御信号はＲＯＭに格納するか、あるいはＣＡによって生成することができる。
・定義：セルが、セル制御信号で制御される場合、それは制御可能なセルである；そうでなければ、それは基本セルである。ＣＣＡは、制御可能なセルおよび基本セルの組み合わせである。制御可能なセルおよび基本セルの双方は、ルール制御信号を有し得る。

【００７８】

制御可能なセルの動作は、その現在のセル制御信号によって決定される。制御可能なセルは、ノーマルとするか（セル制御信号が０である場合）、あるいはアクティブ（セル制御信号が１である場合）にすることができる。制御可能なセルがノーマルな場合、制御可能なセルおよびその近傍の状態の計算は、（現在のルール制御信号およびその近傍の状態によって）通常とおりである。制御可能なセルがアクティブな場合、制御可能なセルおよびその近傍の状態の計算は、いくつかの予め定められた動作によって特定される。制御可能なセルおよびその近傍に適用された動作は相違し得る。予め定められた動作が制御可能なセルの状態計算に影響することになる。

【００７９】

ＣＣＡの構造は、合計でＬ個のセルを有する。Ｍ（Ｍ ≦ Ｌ）セルは、制御可能なセルであり、残りのセルは基本セルである。ここで、基本セルは、すべてプログラム可能なセルである。したがって、このＣＣＡでは、ルール制御ビットおよびセル制御ビットがある。ルール制御ビットを有する、Ｌ－セルのプログラム可能なＣＡ（ＰＣＡ）と比較して、ＣＣＡの追加コストは、Ｍセル制御ビットである。ＣＡ遷移中に、どのルールを、基本および制御可能なセルの双方上で使用すべきか、ルール制御信号が決定し、セル制御信号は、制御可能なセルの状態を決定する。

【００８０】

ＣＣＡの制御可能なセルの使用により、それとプログラム可能なＣＡ（ＰＣＡ）（ルール制御信号だけが存在する）を区別する。一旦制御可能なセルおよび基本セルの動作が特定されれば、制御可能なセルのセッティングは、ＣＣＡの性能を決定する。ＰＣＡとＣＣＡでの共通の概念は、ＣＡ遷移を、より予測不能でより柔軟にするために、ＣＡセルについて、それらが双方とも、いくつかの制御ラインを使用するということである。相違点は、ＰＣＡでは全てのセルが均質な構造を有し、一方、明らかにＣＣＡ中では、制御可能なセルの構造は基本セルのそれと同じではないということである。

【００８１】

同様のＣＡの性能を達成するために、他の方法を使用してもよい。例えば、半径（つまり近傍の数）を増加させたり、各セル中でより多くの状態を使用したり、または各セルのルール・テーブルを発展させたりすることである。コストが比較可能ではないので、との方法が、性能またはハードウェア設計において良いのか言うのは難しい。ルール・テーブルを発展させる代わりに、セル状態を変える場合、異なる計算アプローチを適用することができるように、ＣＡセルの状態を制御するスキームが提案されている。これに基づいて、進行中にセル状態を変更することができるＣＡ－ＣＣＡの新しいクラスは、非特許文献６で提案されている。その研究は、当時良好なランダム性品質を得ることができるＣＣＡの良い構成を見つけることに焦点を絞っていた。

【００８２】

下記では、２つの制御可能なセルタイプが提案されており、これらは、性能をさらに検討するためにＣＣＡの例として用いられる。

【００８３】

上述のように、セル制御信号が０である場合、制御可能なセルは基本セルと同じ動作をとる。一方、セル制御信号が１である場合、制御可能なセルは予め定められた動作を実行する。つまり、ノーマルな場合にそれが行なう動作とは相違し得る。これは、アクティブな場合、制御可能なセルが行なう動作が、制御可能なセルの特性を決定することを意味する。

【００８４】
アクティブにされた制御可能なセルが実行できる最も単純な動作は、ＣＡ計算プロセスの間に、その状態を維持することである。その間に、通常通り、その近傍の状態が計算される。この種の制御可能なセルは、タイプ０の制御可能なセルと呼ばれる。タイプ０の制御可能なセルおよび基本セルの組み合わせであるＣＣＡは、以下ではＣＣＡ０と呼ぶ。
【００８５】
制御可能なセルがアクティブとされた場合、タイプ２の制御可能なセルとなり、その最新の状態を維持するが、その近傍はそれをバイパスする。つまり、これは、アクティブにされた制御可能なセルが、その近傍の状態計算に関係しないということである。このように、近傍関係は、ＣＡ計算プロセスの間に、ダイナミックに変更される。タイプ２の制御可能なセルと基本セルとの組み合わせであるＣＣＡは、ＣＣＡ２または近傍変更ＣＡ（ＮＣＡ）と呼ばれる。その近傍変更挙動のためにＣＣＡ２は、、どんなＰＣＡによってもシミュレートすることができない。
【００８６】
本実施形態による装置および方法：
例えばストリーム暗号のための、本実施形態による新たな構築ブロック・ファミリのデザインに対する基本的な構想には、下記が含まれている。
（１）最近報告されたセルオートマトンと、構築ブロック出力シーケンスの次の２つの特性を制御するための背景技術を与えるＣＡベースの擬似乱数生成器との使用：
・統計特性（ランダム性）、
・周期、
（２）時間変化アルゴリズムを生成に利用することによって、構築ブロック出力シーケンスの非予期性を提供すること、特に下記を提供すること：
・報告された改善された速い相関性攻撃（例えば、非特許文献８参照）および代数的攻撃（例えば、非特許文献９参照）に対する耐性。
【００８７】
構築ブロックは複数の部から構成され、その各々は、次の項目、つまり、長い周期、良好な統計、非予期性のうちの１つまたは２つに寄与する。
【００８８】
本実施形態の設計では、セルオートマトンは主要素として使用される。ＣＡと関連する次の最近の報告が考慮されている。
・非特許文献１および６は、ＣＡ構造を指摘しているが、これらは、非特許文献１１で示した表４中で列挙された多数の統計的テストをパスすることができる高いランダム性のバイナリシーケンスを生成する２Ｄ－ＣＡ（２次元セルオートマトン）およびＣＣＡ（制御可能なセルオートマトン）である。表４はダイハード（DIEHARD）テスト集として知られている。
・非特許文献４中で報告されている結果は、分析上の立証可能性（上記セクションも参照）を有する、最大の周期シーケンスを生成するＣＡ構造を指摘している。
【００８９】

【表４】

インデックス番号	テスト名	グレード
1	Overlapping Sum	
2	Runs up 1	
	Runs Down 1	
	Runs up 2	
	Runs Down 2	
3	3D Sphere	
4	A Parking Lot	
5	Birthday Spacing	
6	Count the Ones 1	
7	Binary Rank 6*8	
8	Binary Rank 31*31	Ｐ値が０又は１ではない場合、合格と見なす。
9	Binary Rank 32*32	
10	Count the Ones 2	
11	Bitstream Test	
12	Craps Wins	
	Craps Throws	
13	Minimum Distance	
14	Overlapping Permutation	
15	Squeeze	
16	OPSO Test	
17	OQSO Test	
18	DNA Test	
18	Overall KS Test	

【００９０】

本実施形態では、次の３つの主要素を構築ブロックに使用することができる：

・図１に表示された、表１中で挙げられた特定の例を有する第１の実施形態の説明において指定された２×Ｌ　ＣＡ

・図２に表示され、表２に基づいた第１の実施形態の説明で指定された２Ｄ－ＣＡ；

・図４～５に表示され、表５中で特定されたＣＣＡ；および

・２×Ｌ　ＣＡ、２Ｄ－ＣＡおよびＣＣＡから結果的に生じるシーケンスのビット毎ｍｏｄ２の合計のための加算器。

【００９１】

【表５】

セルインデックス間隔	1-10	11-20	21-30	31-40	41-50	51-60	61-64
セル更新ルール	0110101111	0010110001	1100101011	1101111011	1100110001	0001000000	1111
セル計算ルール	0000111110	0000011010	1111100010	0101100111	1001010111	1000110111	1101

【００９２】

使用されたＣＣＡ構造は表５で特定されるが、これは、最適化（進化した多目的最適化：evolutionary multi objective optimization:ＥＥＯＯ）アルゴリズムによって得られ、最良の統計特性を有するものの一つとして非特許文献６で報告されている。表５の第２行では、「１」は制御可能なセルを示し、また、第３行では、「１」はＣＣＡ出力に寄与するセルを示す。

【００９３】

図４は、本実施形態の装置でＣＣＡを含む全体的なブロック構造の例を示す。図５（Ｂ）は、ＣＣＡの内部構造の一例を示す。また、図５（Ａ）はＣＣＡを構成するセルユニットの構造の一例を示す。

【００９４】

図４で示すように、本実施形態では、ＣＣＡ４００についてのルール制御信号（ルール制御ワード）およびセル制御信号（セル制御ワード）が、２つのＣＡ４０１，４０２によって別々に生成されると仮定する。ルール制御信号を生成するＣＡ４０１は、ルール制御ＣＡと呼ばれる。セル制御信号を生成するＣＡ４０２は、セル制御ＣＡと呼ばれる。

【００９５】

図５（Ｂ）で示すように、ＣＣＡ４００は、複数個のセルユニット５１０－１，．．．，５１０－ｉ，．．．，５１０－ｊ，．．．，および５１０－Ｌを含んでいる。本例においては、ＣＣＡ４００が、合計でＬ個のセルを有しており、Ｍ（Ｍ ≦ Ｌ）個のセルが制御可能なセル（例えば、セルユニット５１０－ｉ，５１０－ｊ）であり、残りのセルが基本セル（例えば５１０－１，５１０－Ｌ）であると仮定している。制御可能なＣＡセルユニットは、例えば図５（Ａ）で示すように、セル５１０１（その状態は、セル制御信号およびルール制御信号によって制御される）と、左右近傍セルの状態を入力するための加算器５１０２とを有している。

【００９６】

ここで、基本セルは、すべてプログラム可能なセルである。したがって、このＣＣＡには、ルール制御ビットおよびセル制御ビットがある。ルール制御ビットを有する、Ｌセルのプログラム可能なＣＡ（ＰＣＡ）と比較して、ＣＣＡの追加コストはＭセル制御ビットである。ＣＡ遷移中に、制御信号は、どのルールを基本および制御可能なセル上で使用するか決定する。セル制御信号は、制御可能なセルの状態を決定する。

【００９７】

各サイクルで、ＣＣＡセルについてのルール（セル）制御信号のビット組み合わせは、ルール（セル）制御ワードと称される。ルール制御ワードの長さは、ＣＣＡ４００のそれと同じであり、一方、セル制御ワードの長さは、ＣＣＡ４００中の制御可能なセルの数によって決定される。

【００９８】

ＣＣＡ４００のランニングシーケンスは、次のように説明される。初期シードおよび遷移ルールは、それらを初期化するために、ルール制御ＣＡ４００、セル制御ＣＡ４０２およびＣＣＡ４００へ入力される。ＣＣＡセルについて、ルールおよびセル制御ワードを生成するために、２つの制御ＣＡ４０１，４０２が、ＣＣＡ４００と同期して作動する。各サイクルにおいて、ＣＣＡセルの前の状態およびルール／セル制御ワードは、ＣＣＡセルの現在の状態を決定する。いくつかのＣＣＡセルの現在の状態は、出力ビットシーケンスとして、すべてのサイクルで記録される。

【００９９】

非常に多くの研究がＰＣＡでの良好な遷移ルールの探索のために行われているため、非特許文献６では、勧められたルールを選択している。非特許文献６で使用される４つの加法ルールは、ルール９０、１５０、１０５および３０である。ルール９０および１５０は、ＣＣＡ中で遷移ルールとして使用される。これは、１ビットＰＣＡ９０１５０との比較を容易にする。ルール３０はルール制御ＣＡ中で使用され、ルール１０５はセル制御ＣＡ中で使用されるが、これら２つのルールが、非特許文献７によると、乱数発生で最良のものと言われているからである。なお、６４のセルを備えた非特許文献６で記述・使用され

たＣＣＡ（ＣＣＡ２）においては、３５の制御可能なセルおよび３５の出力セルがあり、２０は制御可能なセルである。

【０１００】

本発明の本実施形態によれば、上述の構築ブロック（３－ＣＡ）のファミリを含む装置が提供される。本装置は、制御可能な周期を有する、実用上予測不能な高品質の擬似乱数シーケンスを生成する。

【０１０１】

典型的な３－ＣＡ構築ブロックを備えた装置を、図６に示す。本装置は、２Ｄ－ＣＡ３１０と、２ＸＬ　ＣＡ３２０と、ＣＣＡ４００と、２Ｄ－ＣＡ３１０、２ＸＬ　ＣＡ３２０およびＣＣＡ４００からの対応するセル出力のビット毎ｍｏｄ２加算を行なう加算器６００－１，６００－２，．．．，６００－ｎと、生成した高品質擬似乱数シーケンス６５０を出力するために、ｍｏｄ２加算演算結果をバッファするためのバッファ３４０と、を有する。

【０１０２】

さらに、本実施形態の装置では、２Ｄ－ＣＡ３１０および２ＸＬ　ＣＡ３２０は、ルール制御ＣＡ４０１およびセル制御ＣＡ４０２としてそれぞれ機能する。言いかえれば、ルール制御ワード６１０およびセル制御ワード６２０は、２Ｄ－ＣＡ３１０および２ＸＬ　ＣＡ３２０からそれぞれ生成され、図４および図５で示されるようにセルおよびルール制御用のＣＣＡ４００に供給される。

【０１０３】

図６に示された本装置は、以下のように動作する。

・初期化：独立したランダム・ビットのシーケンスを用いて、すべてのセルを初期化する。

・シーケンス生成：３－ＣＡ構造の装置の各サイクルは、次のステップを含む：

（１）２ＸＬ　ＣＡ　３２０を１サイクル動作させ、その全てのセルを更新する；

（２）２Ｄ－ＣＡ　３１０を１サイクル動作させ、その全てのセルを更新する；

（３）２Ｄ－ＣＡセルに基づいたＣＣＡルール制御ワードを特定する；

（４）２ＸＬ　ＣＡセルに基づいたセル制御ワードを特定する；

（５）ＣＣＡを１サイクル動作させ、その全てのセルを更新する；および

（６）対応するＣＣＡ、２Ｄ－ＣＡおよび２ＸＬ　ＣＡセルのビット毎ｍｏｄ２加算を行なう。

【０１０４】

表６は、使用されたＣＡセルの総数および出力シーケンス周期の得られた下限によって測定された構築ブロック空間複雑度の例を示す。

【０１０５】

【表６】

使用されたＣＡセル数	出力シーケンス周期の下限
128	2^{64}
256	2^{128}

【０１０６】

第３の実施形態：

本発明の第３の実施形態では、暗号の擬似乱数シーケンス生成器（キーストリーム生成器）のファミリは、ストリーム暗号の設計および関連するアプリケーションのために提供される。本実施形態のファミリは、高効率とセキュリティを同時に生む。本実施形態のキーストリーム生成器は、高いランダム特性、長い周期のシーケンスを生むものであり、実

用上予測不能である。

【０１０７】

本実施形態のキーストリーム生成器は、出力擬似乱数シーケンスが所望特性を生むように組み合わせられた、３つの異なるクラスのセルオートマトン、ラテン方格に基づいた非線形マッピングおよび不均一な間引き処理に基づくものである。

【０１０８】

ストリーム暗号用の適切な暗号擬似乱数シーケンス生成器またはキーストリーム生成器の開発は、良く認識されており、開かれた課題である。多くの根本的な要素およびキーストリーム生成器は、関連する技術文献の中で報告されている。報告されたスキームのうちのいくつかは、セルオートマトン（ＣＡ）に基づく。

【０１０９】

元々、セルオートマトン（ＣＡ）は、自己複製の構造を調査するために１９５０年代の初めにフォン・ノイマンによって提案された。ＣＡに基づく擬似乱数発生器（ＰＲＮＧｓ）についての関心の増大は、その単純さおよびカスケード構造のためであり得る。ＣＡは、規則的であり、ローカルに相互連結することができ、そしてモジュール式である。これらの特性のため、ハードウェア中でＣＡをインプリメントすることが、他のモデルよりも簡単になる。ＣＡは、乱数シーケンスを、連続あるいはパラレルのいずれかで生成することができる。実際上、ほとんどのＣＡでは、より高い作業効率を得るために、シーケンスをパラレルに生成する。

【０１１０】

セルオートマトンはセルのアレイであり、各セルは、許容可能な状態のうちの任意の１つをとることができる。各離散時間ステップ（時計サイクル）では、セル状態の変更は、その遷移ルールに依存し、これはｋ近傍ＣＡについて、そのｋ近傍の現在の状態の関数である。セルアレイ（グリッド）は、ｎ次元であるが、ここで、ｎ＝１，２，３が実際上使用される。ＸＯＲおよびＸＮＯＲルールの組み合わせがあるＣＡは、加法的（additive）ＣＡ（非特許文献３）と呼ばれる。ＣＡセルがすべて同じルールに従う場合、ＣＡは均質で（uniform）あると言う；そうでない場合、それは不均一（non-uniform）か、あるいはハイブリッド（非特許文献７）である。ＣＡは、端部のセル（最初のセルおよび最後のセル）が互いに隣接している場合に、周期的境界ＣＡ（ＰＢＣＡ）であると言う。ＣＡは、端部のセルが、その左（右）セル（非特許文献３）のみに接続される場合に、ヌル境界ＣＡであると言う。

【０１１１】

加法的セルオートマトン（Additive Cellular Automata）：

ＣＡの非常に重要なクラスは、ＧＦ（２）における線形ＣＡまたは加法的ＣＡである。次の状態を生成する論理が、ＸＯＲまたはＸＮＯＲ演算だけを使用する場合、ＣＡは加法的ＣＡであると言う。線形のＣＡは、線形の有限状態機械（ＬＦＳＭ）の特定な形である。すべてのＬＦＳＭは、ＧＦ（２）の上の遷移行列によって一義的に(uniquely)表わされ、すべての遷移行列は、固有多項式を有する。

【０１１２】

ＸＯＲ演算だけを備えたＬセルの一次元加法的ＣＡについては、Ｔで示された線形演算子が、ＣＡを特徴づけ得ることが、非特許文献１２の中で示されているが、Ｔは、ＬＸＬブール行列であり、そのｉ番目の行は、ｉ番目のセルの近傍依存性を特定する。ＣＡの次の状態は、列ベクトルとして表わされる現在のＣＡ状態のこの一次演算子を適用することにより生成される。演算は、正規行列乗算であるが、含まれている加算は、モジュール２合計である。ｘ（ｔ）が、ｔ番目の時刻のオートマトンの状態を表わす列ベクトルであれば、オートマトンの次の状態が、以下で与えられる：

$$x(t+1) = T \times x(t)$$

ＣＡの固有多項式がプリミティブな場合、それは最大長ＣＡと呼ばれる。そのようなＬ個のセルからなるＣＡは、全０状態を除き、連続サイクルで$2^{L}-1$の状態すべてを生成する。

【０１１３】
固定次数Ｌについては、２Ｌ**２遷移行列（従って、２Ｌ**２のＬＦＳＭ）があるが、２Ｌ次のＬ多項式だけであるので、次の状況がある：ＬセルＬＦＳＭとＬ×Ｌ行列の間に一対一対応があり、そして同時に、遷移行列とＬ次の多項式の間に多対一の対応がある。
【０１１４】
ＬＦＳＭの固有多項式を得ることは難しくない。というのは、行列式の評価によりそれを計算することができるからである。他方では、特定の固有多項式で特定のタイプのＬＦＳＭ（ＣＡのような）を見つけることは、非特許文献１３の中で解決された課題である。ここでは、与えられた固有多項式を有するＣＡを得るための方法が示されている。当該方法は、各既約多項式について、ＣＡが存在するか否かの課題を解決するためにも使用することができる。
【０１１５】
プログラム可能なセルオートマトン（Programmable Cellular Automata）：
ルール９０およびルール１５０の位置表現は、近傍依存性が単に１つの位置において、すなわちセル自体上で異なることを示している。したがって、１つのセルについて単一の制御線を配することよって、異なる時間ステップに、ルール９０およびルール１５０の双方を同じセルに適用することができる。そのために、Ｌ個のセルＣＡ構造は、２Ｌ個のＣＡ配置を実現するために使用することができる。同じ構造上で異なるＣＡ配置（ルールを更新するセル）を実現することは、適切なスイッチを制御するために、制御論理を使用して達成し得る。また、ＲＯＭに格納された制御プログラムは、制御をアクティブにするために使用することができる。ＲＯＭワードのｉ番目のビットの１（０）状態は、ｉ番目のセルを制御するスイッチを閉じる（開く）。このような構造は、プログラム可能なセルオートマトン（ＰＣＡ）と呼ばれる。
【０１１６】
従って、更新するルールを形成するセル当たり１つの操作量を配して、そのセル（ルール９０あるいはルール１５０の）に適用することができる。ルール９０（１５０）が、ｉ番目のセルに適用される場合、ｎセルＰＣＡのためのｎビット制御ワードは、ｉ番目のセルの上に０（１）を有する。
【０１１７】
セルオートマトンに基づく擬似乱数生成器：
本実施形態が適用されるＣＡの擬似乱数生成器（ＰＲＮＧ）は、研究が盛んな分野であった。非特許文献３は、最大長のＣＡによって生成されたパターンのランダム性が、線形のフィードバック・シフトレジスタ（ＬＦＳＲ）のような他に広く用いられている方法よりも著しくよかったことを示している。
【０１１８】
複数の論文では、あるＰＣＡと同様に一次元の（１－ｄ）ＣＡ ＰＲＮＧも議論された。しかしながら、これらが、まだいくつかのランダム性テストを通らないので、１－ｄＰＣＡでも、ランダム性品質は、完全には満足できるものではない。
【０１１９】
ＣＡのランダム性を改善するために、いくつかのセルに、セル制御信号を加えることにより、１－ｄ ＰＣＡを増強し、かつＣＡの状態を制御するアプローチが報告されている（非特許文献６を参照）。最初の概念は、さらに洗練されて、近傍変更ＣＡ（ＮＣＡ）の概念になった。１－ｄ ＮＣＡに関するランダム性テスト結果は、それらが１－ｄ ＰＣＡよりも良いことを示した。非特許文献６では、１－ｄ ＮＣＡは、最小のコストを備えた最良のパフォーマンスまで進展した。
【０１２０】
他方、代案として、ＣＡ ＰＲＮＧｓのランダム性品質をさらに改善するために、擬似乱数生成に二次元の（２－ｄ）ＣＡを使用するアプローチが報告された。非特許文献１では、非特許文献１１のダイハードテストをパスし得る６４セルの２－ｄ ＣＡを進展させたことが報告されており、これは、現在では、パスするのが最も困難なテスト群であると

言われている。ランダム性テスト結果の比較は、２－ｄ ＣＡがランダム性において、１－ｄ ＮＣＡに匹敵する。しかし、２－ｄ ＣＡの構造の複雑度は、１－ｄ ＣＡと比較して多少高い。

【０１２１】

近年、ＧＦ（２）の上の線形セルオートマトンに基づいた２つのキーストリーム生成器（ＲＯＭおよび２ステージＰＣＡを備えたＰＣＡと呼ばれる）が、それらの安全性分析（security analysis）の結果と共に、非特許文献１４中で提案された。

【０１２２】

他方、中央のＣＡセルによって生成されたビットのシーケンスに基づいたバイナリの非線形のＣＡ初期状態を再構築する方法が、非特許文献１５中で与えられている。ＧＦ（２）上の非線形の遷移ルールおよびＣＡを仮定して、所与の状態のプリデセッサ（predecessor）を計算する転位アルゴリズムが、非特許文献１６中で提案されている。

【０１２３】

２ステージＰＣＡおよびＲＯＭを備えたＰＣＡの暗号の安全性分析は、非特許文献１７および１８の中でそれぞれ報告されており、ここで、ある暗号解読の攻撃のこれらのスキームのいくつかの脆弱性が、暗号文のみの攻撃（ciphertext only attack）と仮定して、実証されている。また、有効な秘密鍵サイズが、その正式の長さより著しく小さいことが示されている。同じ弱点は、既知の平文攻撃（plain text attack）を仮定する非特許文献１９中で指摘されている。

【０１２４】

近年、ＲＯＭを備えたＰＣＡに基づく改善されたキーストリーム生成器が非特許文献２０で、ＧＦ（２）上の演算を仮定して、提案され分析されている。ＧＦ（ｑ）（ｑ＞２）上のＣＡのキーストリーム生成器アプリケーションが非特許文献１０で報告されている。

【０１２５】

本実施形態による装置および方法：

本実施形態によるキーストリーム生成器は、αブロックおよびβブロックと呼ばれる以下の２つの部分を備えている：

・第１の部分αブロックは次を提供する；
　　＊長い周期
　　＊良好な統計
　　＊基本的な非予期性
・第２の部分βブロックは次を提供する；
　　＊増強された最終非予期性。

【０１２６】

αブロックの設計に対する根本的な概念は、次を含んでいる：

（１）最近報告されたセルオートマトンと、構築ブロック出力シーケンスの次の２つの特性を制御するための背景技術を与えるＣＡベースの擬似乱数生成器との使用：
・統計特性（ランダム性）、
・周期、
（２）時間変化アルゴリズムをその生成に利用することによって、αブロック出力シーケンスの非予期性を提供すること、特に下記を提供すること：
・報告された改善された速い相関性攻撃および代数的攻撃に対する耐性。

【０１２７】

αブロックは、複数の部からなる構築ブロックを含むよう構成され、その各部は、次の項目のうちの１つあるいは２つに寄与する：
－長い周期、
－良好な統計、
－非予期性。

【０１２８】

αブロックの構造は、２ＸＬ ＣＡ、２Ｄ－ＣＡおよびＣＣＡを含んでいるが、これは

上述の実施形態に詳細に説明されている。同様の要素は、同じ番号によって指定されるので、その説明は簡単のために省略する。

【０１２９】

βブロックの主な役割は、αブロックからの出力シーケンスの非予期性を増強することにある。

【０１３０】

αブロックからの出力シーケンスが、バッファされ、βブロックによる処理が、次の２つの操作によって行なわれることが考えられる：

・メモリによる非線形関数によるフィルタリング、および

・前のステップから得られたシーケンスの不均一間引き（non-uniform decimation）。

【０１３１】

βブロックで行なわれる処理の例は、図７と図８に示されている。図７は、非線形関数Ｆ１（７０１）およびＦ２（７０２）を使用して、メモリによる非線形マッピングのブロック構造例を示す。バッファ７００は、αブロックからの出力シーケンスを記憶する。図８は、非線形関数Ｆ１（７０１）およびＦ３（７０３）を備えた、不均一の間引きのブロック構造例を示す。間引手段８００は、非線形関数Ｆ３からの出力の制御下で、非線形関数Ｆ１からの出力シーケンスを間引きする。

【０１３２】

図９は、使用された非線形マッピングの一般的な形態の例を示す。使用された関数Ｆ１、Ｆ２およびＦ３の各々は、ラテン方格（ＬＳ）に基づいた一般的な非線形マッピング構造に従う。

【０１３３】

使用された非線形関数の各々は、図９で示されるような複数個のラテン方格テーブルからなる。これらのラテン方格テーブルの各々は、マッピング$\{0,1\}^M \times \{0,1\}^M \rightarrow \{0,1\}^M$を行なう。典型的なケースでは、各非線形関数は、２つのレイヤ（すなわち、レイヤ１、レイヤ２）からなる構造である。レイヤ１は、複数個のラテン方格テーブル９０１－１，９０１－２，．．．，９０１－ｉからなり、レイヤ２は、複数個のラテン方格テーブル９０１－ｊ，．．．，９０１－ｋからなる。

【０１３４】

図８で示される処理では、キーストリーム生成器は、非線形関数Ｆ３（７０３）から出力された間引きワードの重みに応じて、生成されたビットを出力することなく完全なサイクルを複数回行なう。

【０１３５】

図１０は、キーストリーム・シーケンス生成器のブロック構造例を示す。キーストリーム・シーケンス生成器は、次のものを備えている：

－３つの異なるクラスのセルオートマトン３１０，３２０，４００（ＣＡ）；

－ラテン方格に基づいた３つの異なる非線形関数７０１－７０３、つまりＦ１、Ｆ２およびＦ３、Ｆ１とＦ２はメモリを備えた非線形のコンバイナ／フィルタの役割をする；

－基本的なキーストリーム・シーケンスの不均一な間引きブロック８００。

【０１３６】

本実施形態では、ＣＡの３つの異なるクラスとして、２ＸＬ　ＣＡ３２０、２次元ＣＡ（２Ｄ　ＣＡ）３１０および制御可能／プログラム可能なＣＡ（ＣＣＡ）４００が使用される。各ＣＡの詳細な特性は、第１および第２実施形態の説明における該当箇所に上述されている。なお、使用されたセルの総数は、本実施形態におけるファミリパラメータのうちの１つである。

【０１３７】

使用された３つのＣＡが、３－ＣＡと呼ぶ下部構造を形成する。これらの３つのＣＡは、該３－ＣＡ下部構造が結果として下記を生むような方法で組み合わせられている：

－高い非線形（および非予期性）；

－出力シーケンスの周期の保証された下限；

－出力シーケンスの検証された統計特性。

【０１３８】

図１０に示された３－ＣＡ構造は、以下のように作動する：

・初期化：独立したランダム・ビットのシーケンスを用いて、すべてのセルを初期化する。

・シーケンス生成：３－ＣＡ構造の各サイクルは、次のステップを含む：

（１）２×Ｌ　ＣＡを１サイクル動作させ、その全てのセルを更新する；

（２）２Ｄ－ＣＡを１サイクル動作させ、その全てのセルを更新する；

（３）２Ｄ－ＣＡセルに基づいたＣＣＡルール制御ワードを特定する；

（４）２×Ｌ　ＣＡセルに基づいた状態制御ワードを特定する；

（５）ＣＣＡを１サイクル動作させ、その全てのセルを更新する；および

（６）対応するＣＣＡ、２Ｄ－ＣＡおよび２×Ｌ　ＣＡセルのビット毎ｍｏｄ２加算を行なう。

【０１３９】

従って、キーストリーム生成器の動作は、初期化およびキーストリーム生成の２つのステップを含んでいる。

【０１４０】

キーストリーム生成器の初期化は、いずれのキーストリーム生成の前でも必要である。キーストリーム生成器の再同期は、初期化と同じ動作を仮定する。

【０１４１】

初期化の主なステップは、下記のとおりである：

－すべてのＣＡセルの初期値を設定すること；

－いかなる出力もなしに、キーストリーム生成器をＭ回動作させる、ここで、Ｍはキーストリーム生成器ファミリのパラメータである。

【０１４２】

次に、各作動サイクルでは、キーストリーム生成器内のキーストリーム生成の主な動作が実行される。キーストリーム生成には、次のものが含まれる：

（１）すべてのＣＡの更新；

（２）非線形関数出力の生成；

（３）間引きルールに応じて、ステップ（４）に行くか、またはステップ（１）および（２）を繰り返す；および

（４）出力シーケンスブロック（キーストリームブロック）の生成。

【０１４３】

上述のように、本実施形態によるキーストリーム生成器は、広い範囲における特定のインプリメンテーションまたはアプリケーション制約に好適な、あるファミリメンバを選択できるという可能性を与えている。本実施形態のキーストリーム生成器は、ハードウェア・インプリメンテーションに、および極めてランダムで、長い周期、および実用上は予測不能なシーケンスを要求する様々なアプリケーションに特に好適である。

【０１４４】

第４の実施形態：

本発明の第４の実施形態によれば、上述の実施形態のうちの任意の１つによる擬似乱数生成器を使用して、暗号処理を行なうことができる装置が提供される。

【０１４５】

図１１は、上記装置の一例を示す。本装置は、コンピュータシステムあるいはＩＣモジュールのような情報処理装置で実現され得る。本装置は、例えば、上述の実施形態のうちの１つに従った擬似乱数生成器（ＰＲＮＧ）１１００、ＣＰＵ１１０１、Ｉ／Ｏインタフェース１１０２、メモリ１１０３、暗号プロセッサ１１０４およびバス１１０５を備えている。

【０１４６】

ＣＰＵ１１０１は、暗号処理の制御、データ送信／受信、構成するユニット間でのデー

タ転送など、様々なオペレーションやプログラムを実行する。メモリ１１０３は、ＣＰＵ１１０１によって実行されるプログラムおよび固定オペレーションパラメータを格納するＲＯＭ、および、記憶エリアおよび／またはプログラムを実行したりパラメータの変更に使用されるワークエリアとして使用されるＲＡＭを含んでいる。さらに、メモリ１１０３は、鍵データなどのようなセキュリティデータを格納するためにセキュア記憶領域を含んでいてもよいが、これは暗号の処理に必要である。改ざん防止（anti-tamper）構造を有するそのようなセキュア記憶領域を形成することは望ましい。

【０１４７】

暗号プロセッサ１１０４は、ストリーム暗号処理および／または解読処理のような暗号処理を行なう。また、暗号プロセッサ１１０４は、ＲＯＭに暗号処理プログラムを予め格納し、ＣＰＵ１１０１にプログラムを読み取らせ実行させることにより実現してもよい。

【０１４８】

ＰＲＮＧ１１００は、暗号処理用の鍵の生成に必要な擬似乱数を生成する。ＰＲＮＧ１１００は、ＣＡに基づくものであり、図３、６および１０で示される構造のうちのいずれか１つであってもよい。

【０１４９】

Ｉ／Ｏインタフェース１１０２は、外部装置とのインタフェースをとり、例えば使用されるべき鍵を指定する情報の入力を受け、該鍵に基づいた暗号文データを出力する。また、Ｉ／Ｏインタフェース１１０２は、メディアリーダ／ライタまたはＩＣモジュールのような外部装置または他の装置とデータ通信を行うデータ通信装置であってもよい。

【０１５０】

なお、添付のクレームあるいはその均等物の範囲内である限り、種々の変更、組み合わせ、下位組み合わせおよび変更が、設計必要条件および他の要因に依存して生じ得ることは、当業者に理解され得るものである。

【図面の簡単な説明】

【０１５１】

【図１】２×Ｌセルオートマトンの一例を示す模式図である。

【図２】二次元のセルオートマトン（２Ｄ－ＣＡ）の一例を示す模式図である。

【図３】本発明の第１の実施形態による擬似乱数シーケンス生成器の構成例を示す模式図である。

【図４】制御可能なセルオートマトン（ＣＣＡ）のマクロブロック構成例を示す模式図である。

【図５】図５（Ａ）および図５（Ｂ）は、ＣＣＡ中の要素の構成例を示す模式図である。

【図６】本発明の第２の実施形態による擬似乱数シーケンス生成器の構成例を示す模式図である。

【図７】本発明の第３の実施形態による、メモリを備えた非線形マッピングのブロックスキームである。

【図８】本発明の第３の実施形態による、不均一な間引きのブロックスキームである。

【図９】ラテン方格に基づいた非線形マッピングの典型的な形式を示す模式図である。

【図１０】本発明の第３の実施形態による擬似乱数シーケンス生成器の構成例を示す模式図である。

【図１１】本発明の第４の実施形態による暗号処理装置の構成例を示す模式図である。

【符号の説明】

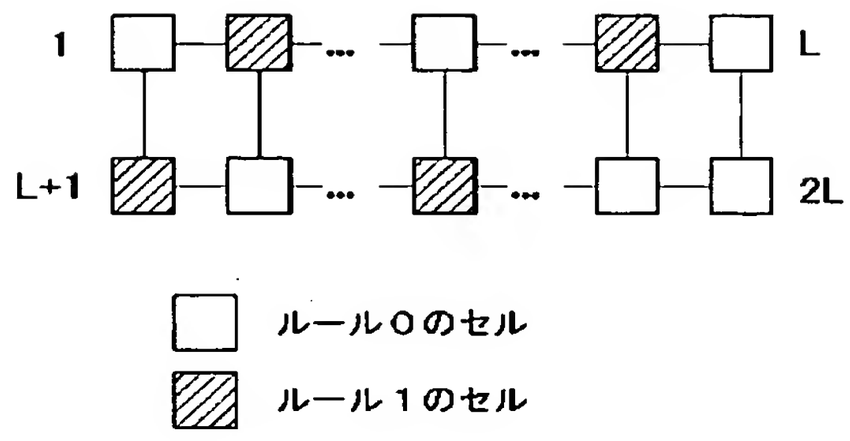
【０１５２】

３１０：二次元セルオートマトン

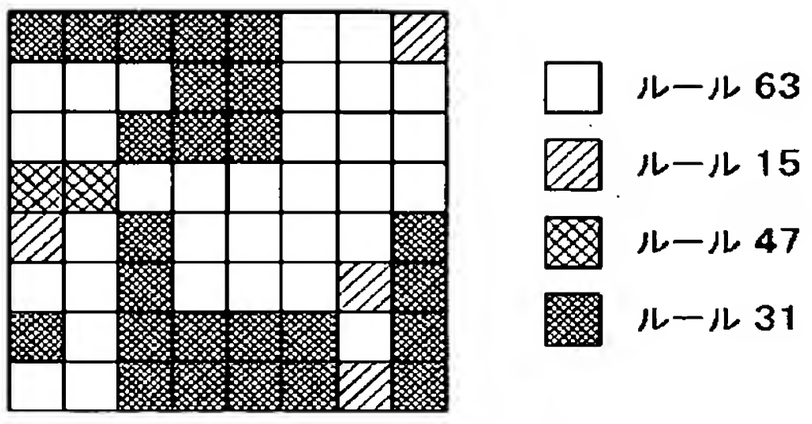
３２０：２×Ｌセルオートマトン

４００：制御可能なセルオートマトン
７０１～７０３：非線形関数

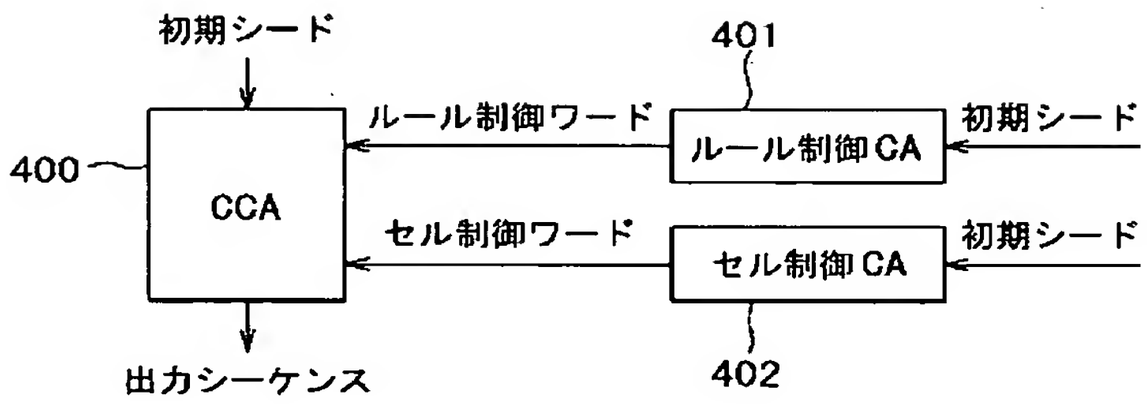
【書類名】 図面
【図１】



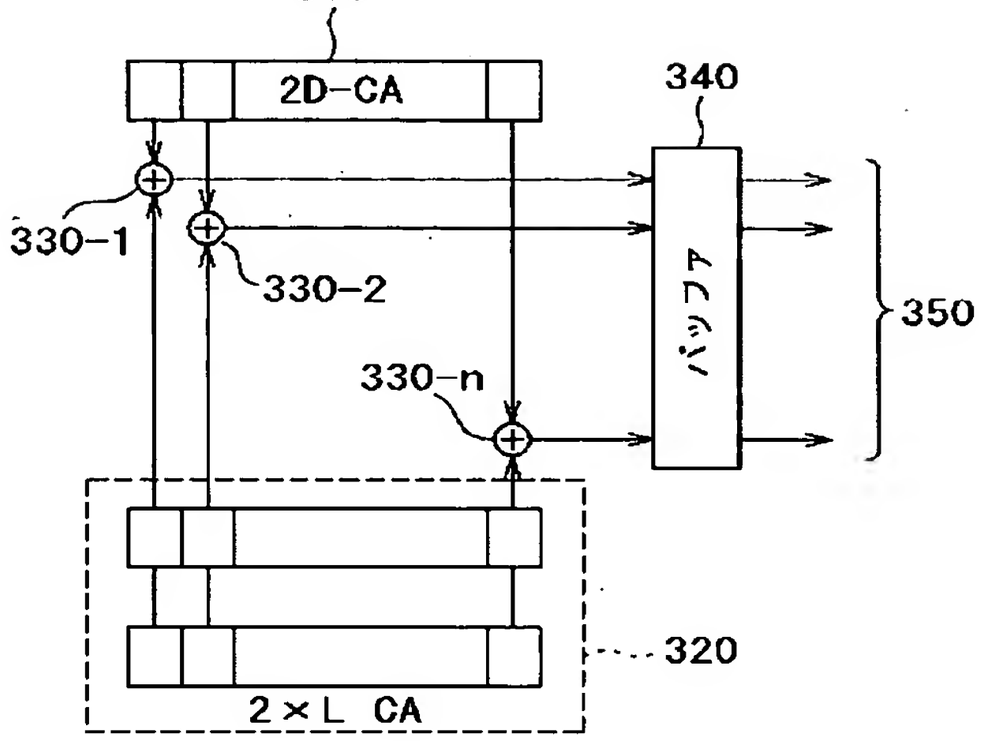
【図２】



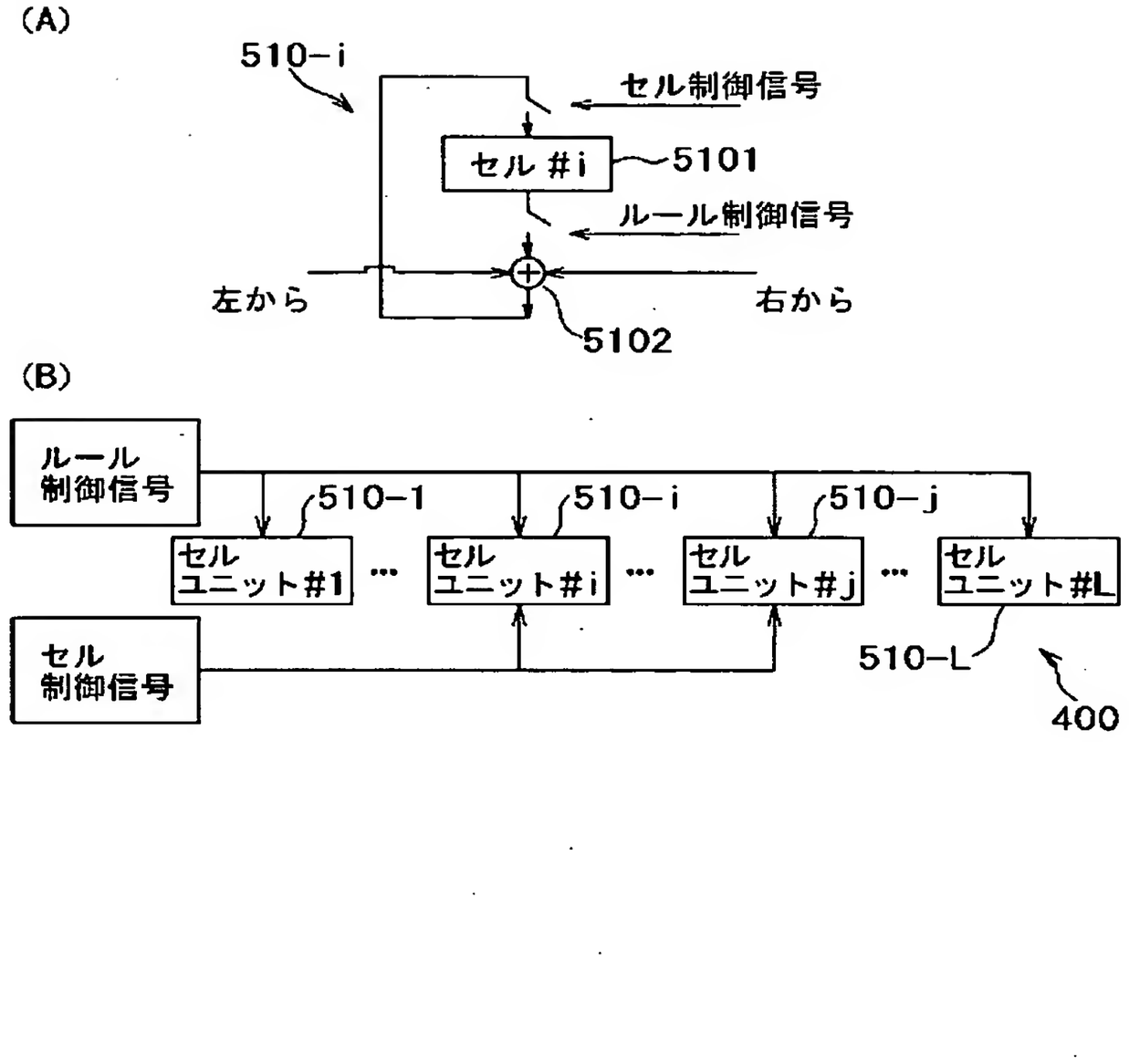
【図３】


初期シード
401
ルール制御ワード
初期シード
400
CCA
ルール制御CA
セル制御ワード
初期シード
セル制御CA
出力シーケンス
402

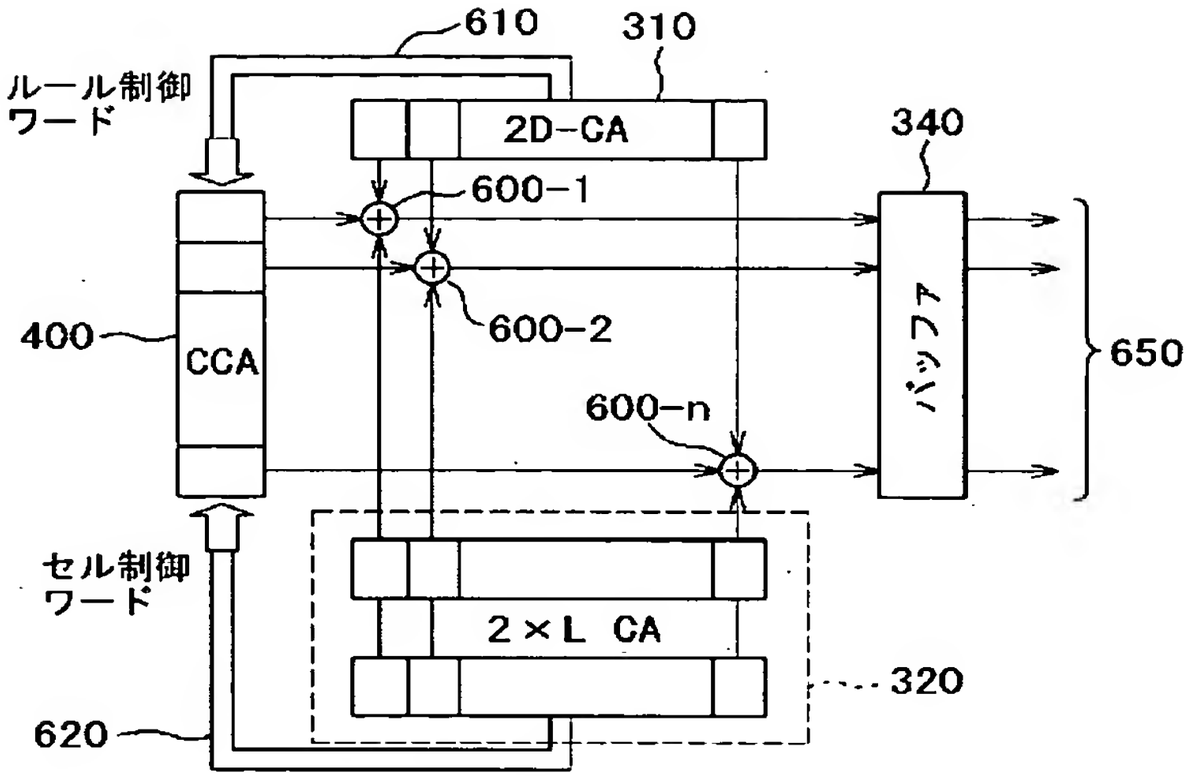
【図４】



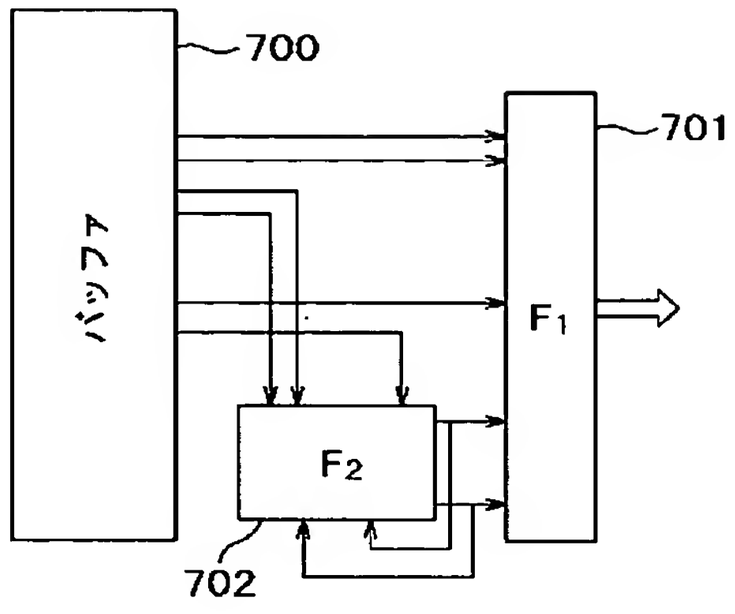
【図５】


(A)
510−i
セル制御信号
セル #i
5101
ルール制御信号
左から
右から
5102
(B)
ルール
制御信号
510−1
510−i
510−j
セル
ユニット#1
セル
ユニット#i
セル
ユニット#j
セル
ユニット#L
セル
制御信号
510−L
400

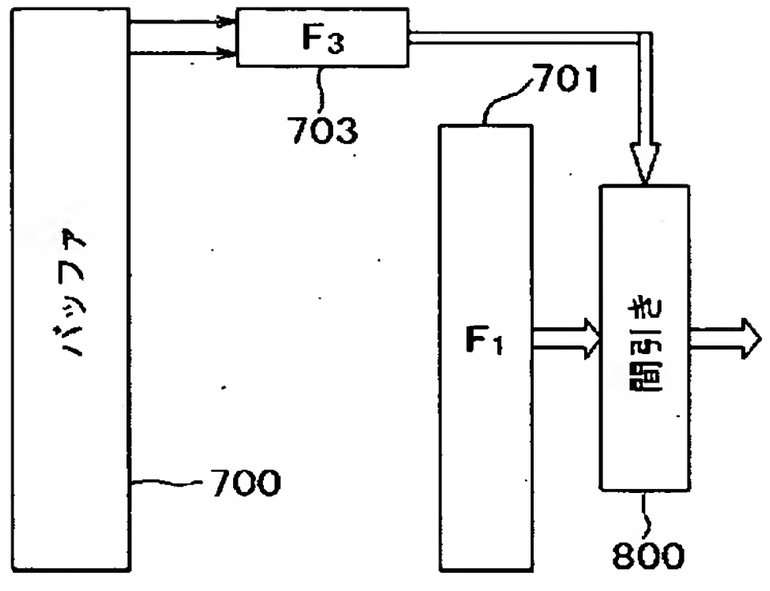
【図６】


610
310
ルール制御
ワード
2D-CA
340
600-1
600-2
400
CCA
バッファ
650
600-n
セル制御
ワード
2×L CA
320
620

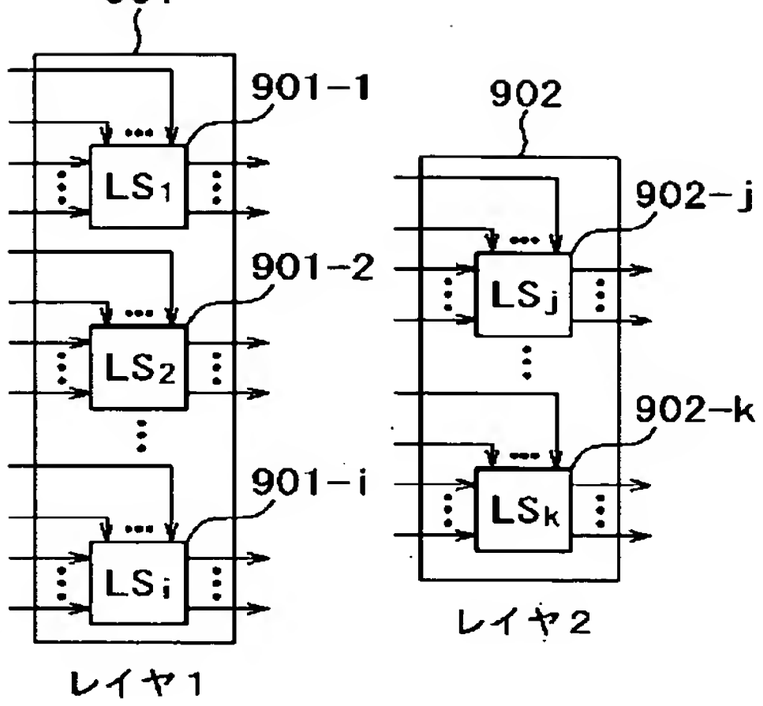
【図７】



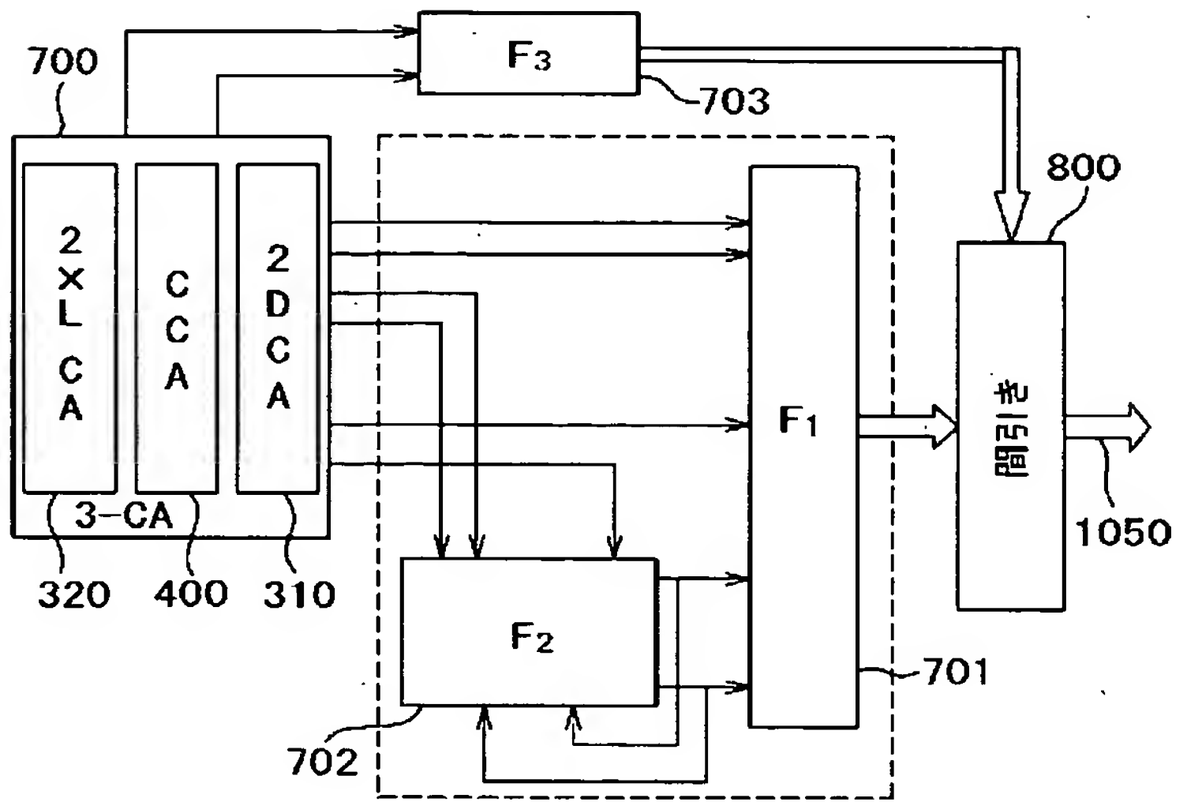
【図８】



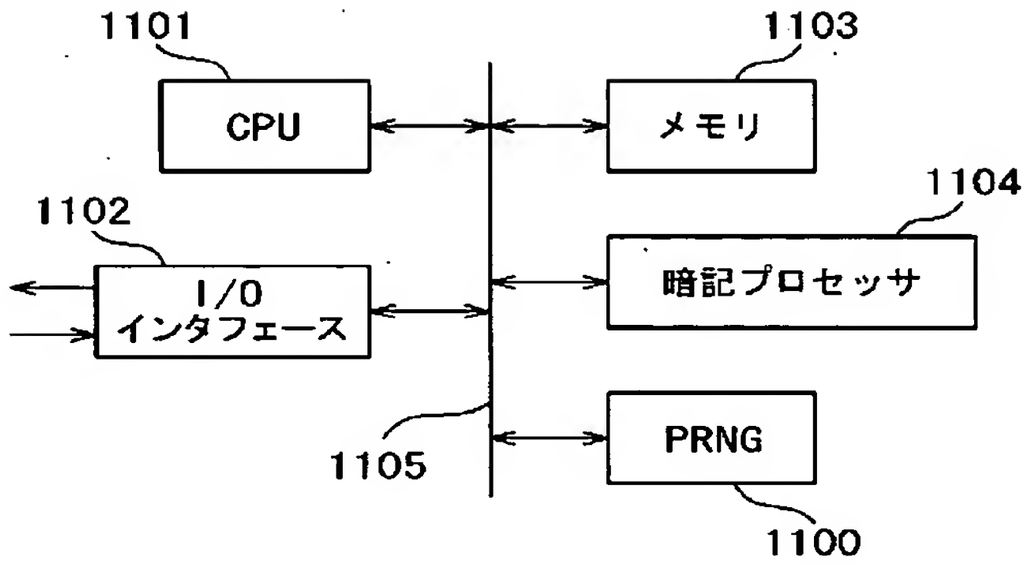
【図９】



【図１０】


700
F3
703
800
2XLCA
CCA
2DCA
3-CA
320
400
310
F1
間引き
1050
F2
701
702

【図１１】


1101
CPU
1103
メモリ
1104
暗記プロセッサ
1102
I/O
インタフェース
1105
PRNG
1100

【書類名】要約書
【要約】
【課題】本発明の目的は、制御可能な周期を有する所望の擬似乱数シーケンスを生成するためのコンパクトな装置を提供することである。
【解決手段】擬似乱数シーケンスを生成する装置は、第１のシーケンスを生成する二次元のセルオートマトン３１０、第２のシーケンスを生成する２×Ｌセルオートマトン３２０、第１のシーケンスおよび第２のシーケンスのビット対ビットｍｏｄ２の和を得るための加算器３３０－１，３３０－２，．．．，３３０ｎ、および加算器３３０－１，３３０－２，．．．，３３０－ｎから結果として得られたシーケンスをバッファするためのバッファ３４０を備えている。
【選択図】　図３

出願人履歴

０００００２１８５
19900830
新規登録
５９７０６２９９３

東京都品川区北品川６丁目７番３５号
ソニー株式会社